PB82-177759

Contractor Requirements for the Control and Security of TSCA (Toxic Substances Control Act) Confidential Business Information

(U.S.) Environmental Protection Agency
Washington, DC

Oct 81

U.S. Department of Commerce
National Technical Information Service
NTIS

BIBLIOGRAPHIC INFORMATION

PB82-177759

Contractor Requirements for the Control and Security of TSCA (Toxic Substances Control Act) Confidential Business Information.

Oct 81

PERFORMER: Environmental Protection Agency, Washington, DC. Office of Toxic Substances.

These procedures prescribe minimum standards and establish responsibility and accountability for the control and security of documents and computer systems that contain confidential business information (CBI) received under the Toxic Substances Control Act (TSCA) and furnished to a contractor to perform work under an EPA contract.

KEYWORDS: *Contractors, *Data processing security, *Computer information security, *Confidentiality.

Available from the National Technical Information Service, Springfield, Va. 22161

PRICE CODE: PC A03/MF A01

EPA-560/--82-002

PB82-177759

CONTRACTOR REQUIREMENTS FOR THE CONTROL AND SECURITY OF TSCA CONFIDENTIAL BUSINESS INFORMATION

October 1981

United States Environmental Protection Agency
Washington, D.C. 20460

REPRODUCED BY
NATIONAL TECHNICAL
INFORMATION SERVICE
U.S. DEPARTMENT OF COMMERCE
SPRINGFIELD, VA 22161

Preface

Contractor Requirements for the Control and Security of TSCA Confidential Business Information deals with a serious obligation EPA contractors have under the Toxic Substances Control Act (TSCA)--the need to protect TSCA Confidential Business Information from unauthorized disclosure. It outlines security requirements that must be met by all EPA contractors who will receive TSCA Confidential Business Information.

TSCA requires industry to entrust large amounts of data to EPA concerning the tens of thousands of chemical substances in U.S. commerce. This information has never been compiled in such a complete way before, and it forms the basis for EPA's ability to carry out TSCA's preventive approach to minimizing the health and environmental risks of toxic chemicals. EPA in turn must often entrust these data to our contractors.

Some of these industry data are claimed as "confidential," meaning that they involve trade secrets or other kinds of information that one company doesn't want another to have. Understandably, industry has expressed great concern about EPA's ability to protect confidential business information from unauthorized disclosure.

It is vitally important to the successful implementation of TSCA that confidential business information submitted to EPA by industry not be disclosed in an unauthorized manner, either by Agency employees or contractors. To ensure that this doesn't happen, EPA has developed strict security procedures to protect TSCA Confidential Business Information and has developed a training program to familiarize all EPA employees with their responsibilities and with the consequences of failure to comply with the security procedures. EPA's basic security requirement for its contractors is that they provide at least the same degree of protection for TSCA Confidential Business Information as EPA does.

The EPA Data Security Task Force has developed these Contractor Security Requirements after reviewing suggestions and comments from throughout EPA and from the public, including contractors themselves. I believe that these requirements properly balance the need for data security with the need for access to the data.

However, any security system is only as good as the people who maintain it. It takes all of us working together to make it succeed. Any one of us acting carelessly or negligently would cause us to fail. Therefore, employees must study and learn the procedures developed by their companies and approved by EPA.

While I don't wish to overemphasize this point, TSCA provides strict criminal penalties for any person who discloses this confidential business information in a knowing and unauthorized way. EPA has gone on public record with the promise to prosecute any acts of wrongful disclosure to the fullest extent of the law.

We are counting on our contractors to help us make this system work.

July 29, 1981
Date

Warren R. Muir
Deputy Assistant Administrator
for Toxic Substances

Contents

	Page
PREFACE	iii
GLOSSARY OF ACRONYMS	vii
BASIC REQUIREMENT	ix
I. GENERAL	1
A. Purpose	1
B. Policy	1
C. Penalties for Violations	1
D. Security Violation	2
E. Procedures for Handling Security Violations	2
F. Definitions	2
II. RESPONSIBILITIES	5
A. Deputy Assistant Administrator for Toxic Substances (DAA/OTS)	5
B. Division Directors	5
C. Contracts Management Division	5
D. Project Officers	6
E. Office of the Inspector General	6
F. Director, Management Information and Data Systems Division	6
G. Contractor Document Control Officers	7
H. Contractor Employees	8
III. PROCEDURES FOR AWARD OR MODIFICATION OF CONTRACTS INVOLVING THE USE OF TSCA CBI	9
IV. CONTRACTOR SECURITY PROCEDURES	11
A. Security Plans	11
B. Transfer of TSCA CBI to Contractor	16
C. Notification of Affected Business	16
D. Audits	17
E. Termination Inventory	17
F. Physical Security	17
G. Contractor Acquired CBI	17
H. Return of CBI to EPA	17
I. Additional Requirements	17

Contents (cont.)

		Page
V. COMPUTER SECURITY		19
	A. Special Rules for Contractor Computer Use	19
	B. Security Requirements for Contractor Computer Centers	20
APPENDIX I:	TREATMENT OF CONFIDENTIAL BUSINESS INFORMATION	25
APPENDIX II:	SECURITY REQUIREMENTS FOR HANDLING TSCA CONFIDENTIAL BUSINESS INFORMATION	27
APPENDIX III:	COMPUTER SECURITY	29
APPENDIX IV:	SCREENING BUSINESS INFORMATION FOR CLAIMS OF CONFIDENTIALITY	31
APPENDIX V:	TSCA CONTRACTOR EMPLOYEE CONFIDENTIALITY AGREEMENT	33
APPENDIX VI:	CONFIDENTIALITY AGREEMENT FOR CONTRACTOR EMPLOYEES UPON TERMINATION OR TRANSFER	35
APPENDIX VII:	REQUEST FOR APPROVAL OF CONTRACTOR ACCESS TO TSCA CONFIDENTIAL BUSINESS INFORMATION	37
INDEX		41

Glossary of Acronyms

AA/OPTS	Assistant Administrator for Pesticides and Toxic Substances
ADP	Automated Data Processing
CBI	Confidential Business Information
CMD	Contracts Management Division
CFR	*Code of Federal Regulations*
DAA/OTS	Deputy Assistant Administrator for Toxic Substances
DCA	Document Control Assistant
DCO	Document Control Officer
DOJ	Department of Justice
EPA	United States Environmental Protection Agency
FSSD	Facilities and Support Services Division
IAG	Interagency Agreement
MIDSD	Management Information and Data Systems Division
OGC	Office of General Counsel
OIG	Office of the Inspector General
OPTS	Office of Pesticides and Toxic Substances
TSCA	Toxic Substances Control Act

Basic Requirement

EPA's basic security requirement for its contractors* is that they provide at least the same degree of protection of TSCA Confidential Business Information as that described in EPA's *TSCA Confidential Business Information Security Manual*.

It is vitally important to the successful implementation of the Toxic Substances Control Act (TSCA) that EPA ensure that TSCA CBI is not disclosed in an unauthorized manner.

EPA has developed strict security procedures to protect TSCA CBI and has developed a training program to familiarize all EPA employees with their responsibilities and with the consequences of failure to comply with the requirements of the *TSCA Confidential Business Information Security Manual*.

Our contractors must meet the same high standards we set for ourselves.

---

*Note: For the purposes of this document, "contractor" shall mean contractor or subcontractor and "contract" shall mean contract or subcontract.

I. General

A. Purpose

These procedures prescribe minimum standards and establish responsibility and accountability for the control and security of documents and computer systems that contain confidential business information (CBI) received under the Toxic Substances Control Act (TSCA) (15 U.S.C. § 2601 et seq.) and furnished to a contractor to perform work under an EPA contract.

B. Policy

EPA recognizes the trust placed in it by the submitters of TSCA Confidential Business Information. It is the policy of EPA to take all reasonable measures to prevent the unauthorized disclosure of such information. EPA contractors are prohibited from disclosing any TSCA CBI except in accordance with the terms of the contract under which they receive the information. TSCA CBI is to be held in confidence and handled in accordance with contractor security procedures approved by EPA.

EPA furnishes TSCA CBI to EPA contractors only when such information is necessary for the performance of the work specified in the contract. Disclosures to contractors will be made only when the procedures in 40 CFR Part 2 have been followed, when the contract contains the required clauses, and when the procedures set forth in this document have been followed.

C. Penalties for Violations

Unauthorized disclosure of TSCA CBI may subject a contractor employee to criminal penalties under TSCA Section 14(d) as follows:

> Criminal Penalty for Wrongful Disclosure--
>
> (1) Any officer or employee of the United States or former officer or employee of the United States, who by virtue of such employment or official position has obtained possession of, or has access to, material the disclosure of which is prohibited by subsection (a), and who knowing that disclosure of such material is prohibited by such subsection, willfully discloses the material in any manner to any person not entitled to receive it, shall be guilty of misdemeanor and fined not more than $5,000 or imprisoned for not more than one year, or both. . . .
>
> (2) For the purposes of paragraph (1), any contractor with the United States who is furnished information as authorized by subsection 14(a)(2), and any employee of such contractor, shall be considered to be an employee of the United States.

Also, violations of these procedures by contractor employees may result in removal from the Authorized Access List and disciplinary action with penalties up to and including dismissal, under conduct and discipline policies and procedures that must be developed by the contractor.

D. Security Violations

If a contractor discovers or has reason to believe that there has been a violation of the contractor security provisions, the contractor DCO must report the circumstances to the EPA Project Officer who will report the suspected violation to the OIG and Chief, ICB. The contractor must allow representatives of EPA to investigate such violations and must cooperate fully and ensure the cooperation of its employees.

E. Procedures for Handling Violations

Upon receipt of any allegation that a contractor or contractor employee has violated procedural requirements under the terms of the contract concerning security of TSCA CBI, the OIG shall initiate an investigation.

In those cases of violation of contract security provisions where there is no evidence of a criminal violation, the OGI shall report the results of the investigation to the DAA/OTS, CMD, and OGC. The DAA/OTS shall, in conjunction with CMD and OGC, initiate appropriate action under the terms of the contract and in accordance with 40 CFR Part 2.

If the investigation by the OIG indicates that a criminal violation has been committed, the investigation shall be referred to the Department of Justice. When the Department of Justice assumes investigative jurisdiction, any further action, including notification to the business making the claim of CBI, will be dictated by them.

The DAA/OTS, in concert with OGC and CMD, shall notify the affected business of the circumstances and the firm's legal rights under the contract in all cases except those referred to the Department of Justice. The cases referred to the Department of Justice require that Department's approval prior to the release of any of the investigative data to the business.

F. Definitions

Access is the ability and opportunity to gain knowledge of TSCA Confidential Business Information (in any manner whatsoever).

An *ADP Application Security Plan* is a formal documented plan that addresses the administrative, technical, and physical controls required during each phase in the life cycle of an application system processing TSCA CBI.

An *Authorized Computer Facility* is an EPA or contractor computer facility that meets EPA security standards.

An *Authorized Person* is any employee authorized by the contractor for access to TSCA CBI.

A *Computer Center Security Plan* is a formal documented plan that addresses the administrative, technical, and physical controls required to protect TSCA CBI within the data center.

Confidential Business Information is any information in any form received by EPA or an EPA contractor from any person, business, partnership, corporation, or association; local, State, or Federal agency, or foreign government that contains trade secrets or commercial or financial information, that has been claimed as confidential by the person submitting it, and that has not been determined to be nonconfidential under the procedures in 40 CFR Part 2.

A *Contractor* is any person, association, partnership, corporation, business, educational institution, governmental body, or other entity performing work for EPA under a contract with EPA. In this document "contractor" means contractor or subcontractor.

A *Contractor Computer Document Control Officer* is a document control officer (DCO) within a contractor computer facility responsible for the security and control of TSCA CBI contained in the computer facility.

A *Contractor Document Control Officer* is a person appointed by a contractor who is responsible for the security, control, and distribution of all TSCA CBI in the possession of the contractor.

A *Document* is any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing card decks, printouts, and tapes; maps; charts; paintings; photographs; drawings; engravings; sketches; samples; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.

A *Document Control Number* is the unique number assigned by an EPA Document Control Officer (DCO), a contractor DCO, or through computer system numbering to a document containing TSCA CBI.

A *Document Control Officer (EPA)* is a person designated in accordance with the requirements of the *TSCA Confidential Business Information Security Manual* to be responsible for the security, control, and distribution of all TSCA CBI received by him/her.

Information is knowledge that can be communicated by any means.

The *Project Officer (EPA)* is the person responsible for serving as coordinator in all matters relating to the security, control, and distribution of TSCA CBI during the performance of a contract.

A *Secure Facility* is a building or portion of a building that meets the requirements of this Manual for handling TSCA Confidential Business Information and has been approved by the Information Central Branch (ICB).

A *Secure Room* or area is a room or area which meets the requirements of this Manual for storage and/or use of TSCA CBI and has been approved by the ICB.

A *Security Plan* is a set of security procedures developed by a contractor and approved by ICB that provides at least the same degree of protection as EPA's *TSCA Confidential Business Information Security Manual*.

A *Violation* is the failure to comply with any provision in the contractor security plan whether or not such failure leads to actual unauthorized disclosure of TSCA Confidential Business Information.

II. Responsibilities

A. Deputy Assistant Administrator for Toxic Substances (DAA/OTS)

The DAA/OTS is responsible for approving all contractors who will receive TSCA CBI, and for approving the Computer Center Security Plans and ADP Security Plans submitted by those contractors.

In the event of violations, the DAA/OTS shall take appropriate action in all cases in which there is no evidence of criminal violation. In all cases except those referred to the Department of Justice, the DAA/OTS shall notify, in concert with OGC and CMD, the affected business of the circumstances and the business' legal rights under the contract. The cases referred to the Department of Justice require that Department's approval prior to the release of any of the investigative data to an affected business.

B. Division Directors

Division Directors are responsible for initiating requests for contractors to have access to TSCA CBI, subject to the approval of the DAA/OTS. The form, Request for Approval of Contractor Access to TSCA Confidential Business Information (Appendix VII), is filled out for this purpose. Division Directors also appoint a project officer for each contract involving the use of TSCA CBI.

C. Contracts Management Division (CMD)

The Director, CMD, Cincinnati; the Director, CMD, Research Triangle Park; and the Chief, Headquarters Contract Operations, under the overall supervision of the Director of the Contracts Management Division, share the responsibility for administering procurement actions and contracts under which TSCA CBI is to be furnished to a contractor to perform specific work.

They must ensure that the proper clauses and provisions are included in all contracts or RFPs that would involve access to or handling of TSCA CBI:

- The Treatment of Confidential Business Information clause (Appendix I), the Security Requirements for Handling TSCA Confidential Business Information clause (Appendix II), and any other clauses requested by a program office must be included in any contract or RFP that would involve the handling of TSCA CBI.

- The Computer Security clause (Appendix III) must be included in any contract or RFP that would involve the introduction of TSCA CBI into a contractor's computer.

- The Screening Business Information for Claims of Confidentiality clause (Appendix IV) must be included in any contract or RFP in which

a contractor would be required to collect CBI directly from a business.

- The proper provisions must be included in any RFP for a contract that permits contractor access to TSCA CBI.

- CMD also evaluates proposals submitted by offerors or contractors and evaluates any potential organizational conflicts of interest that might preclude handling of TSCA Confidential Business Information. In their evaluation, they will take into consideration the offeror's or contractor's past performance on similar contracts that involved the handling of CBI or other information of a sensitive nature, such as national defense information or privacy information.

D. Project Officers

EPA Project Officers are responsible for coordination between elements of EPA and the contractor on matters relating to the security and control of TSCA CBI during the performance of the contract. They also assist CMD in considering possible conflicts of interest and past performance on similar contracts by the contractor or offeror.

Project Officers are also responsible for ensuring that the contractor is ready to be inspected prior to OIG performing the inspections, arranging for the transfer of the data to the contractor, and reporting all alleged violations of contract security provisions to his/her Division Director, OIG, and ICB.

E. Office of the Inspector General (OIG)

The OIG has the inspection and review responsibility for all contractors and offerors involved in the receipt, handling, and storage of TSCA CBI. Personnel from OIG:

- Review contractor security plans

- Inspect contractor facilities prior to the receipt of TSCA CBI and on a periodic basis, announced and unannounced, thereafter to ensure compliance with security requirements

- Review employee training programs as specified in Chapter IV.

- Investigate alleged wrongful disclosures of TSCA CBI and certain other serious violations by the contractor. If such investigation discloses that a possible criminal violation has occurred, the matter will be referred to the Department of Justice.

F. Director, Management Information and Data Systems Division (MIDSD)

The Director of the Management Information and Data Systems Division (MIDSD) will, upon request, review and comment on contractor ADP application security

plans, and assist the OIG in conducting inspections of contractor computer facilities for compliance with security requirements.

G. Contractor Document Control Officers

Contractor Document Control Officers (DCOs) are responsible for controlling TSCA CBI in the possession of the contractor. Specifically, their responsibilities include:

- Serving as a contact person for EPA regarding the security and control of TSCA CBI while it is in the possession of the contractor.
- Conducting periodic audits of the contractor's security system.
- Maintaining a list of contractor personnel who are authorized for access to TSCA CBI, including those authorized for computer access, and releasing TSCA CBI only to such persons.
- Keeping on file in a secure manner a record of the locations and combinations of all locks, safes, and cabinets that contain TSCA CBI, and ensuring that such combinations are changed annually or whenever anyone who knows the combination terminates or transfers, whichever comes first.
- Obtaining a signed TSCA Contractor Employee Confidentiality Agreement (Appendix V) from each contractor employee who will have access to TSCA CBI before the employee is granted access.
- Obtaining a signed Confidentiality Agreement for Contractor Employees Upon Termination or Transfer (Appendix VI) for any employee who terminates or transfers to a position not requiring access to TSCA CBI.
- The original of this form will be forwarded to the Information Control Branch and will be the basis for removing the individual from the EPA TSCA CBI Access List.
- Logging all TSCA CBI received or generated, including computer-generated printouts.
- Assigning document control numbers, attaching cover sheets, and properly marking all documents containing TSCA CBI whenever these things have not already been done.
- Releasing TSCA CBI only to employees authorized for access.
- Ensuring that TSCA CBI is properly stored when not in use.
- Authorizing and supervising the reproduction and destruction of TSCA CBI.

- Reporting all alleged violations of contractor security procedures to the EPA Project Officer immediately.

- Maintaining a copy of the EPA-provided TSCA CBI Access List.

H. Contractor Employees

Contractor employees are responsible for the control and security of all TSCA CBI received by them. Specifically, their responsibilities include:

- Discussing TSCA CBI only with authorized employees of the contractor or of EPA.

- Storing TSCA CBI as specified in Chapter IV.A.3 of this document when not in use or at the close of business.

- Safeguarding TSCA CBI when in actual use as specified in Chapter IV.A.5 of this document.

- Safeguarding combinations to locks, safes, and rooms that secure TSCA CBI.

- Reporting alleged violations of the security procedures to the contractor DCO.

- Giving all TSCA CBI to the contractor DCO for reproduction or destruction and recording in the appropriate log.

- Refraining from discussions of TSCA CBI on the telephone except with the permission of and following guidelines provided by the EPA Project Officer.

III. Procedures for Award or Modification of Contracts Involving the Use of TSCA CBI

The step-by-step procedure described here must be followed for a contractor to become authorized for receipt of TSCA CBI.

1. When an EPA program office decides to initiate a contract (or to modify an existing contract) that will require contractor access to TSCA CBI to perform the work, the appropriate Division Director or equivalent (or above) must request approval for such access from the DAA/OTS using the form, Request for Approval of Contractor Access to TSCA Confidential Business Information (Appendix VII). The DAA/OTS will approve or disapprove the request and notify the requester.

2. If the DAA/OTS approves the request, the Project Officer will send a copy of the approval to CMD. This will be CMD's signal to include in the RFP (or modification) this document, *Contractor Requirements for the Control and Security of TSCA Confidential Business Information*, including the following contract clauses, as appropriate:

   - Treatment of Confidential Business Information (Appendix I).
   - Security Requirements for Handling Confidential Business Information (Appendix II).
   - Computer Security (Appendix III).
   - Screening Business Information for Claims of Confidentiality (Appendix IV).

3. Offerors (or contractors, in the case of modifications) will submit Security Plans to CMD, who will, in turn, submit them to the OIG. The OIG will review the plans to determine if they meet the minimum requirements of this Manual and forward them to ICB. No technical evaluation (in the case of offerors) will be done until the security plan is approved by the ICB.

4. In evaluating the proposals, CMD and the program office will evaluate any potential organizational conflicts of interest that might preclude handling of TSCA CBI by the offeror. They will also consider the offeror's past performance on similar contracts that involved the handling of CBI or other information of a sensitive nature, such as national defense information or privacy information.

5. ICB will approve or disapprove the security plan. In the case of an offeror, if the security plan is rejected, no technical evaluation will be done. In the case of a modification to an existing contract, if there are only minor problems with the security plan, the project officer will work with the contractor to correct them. If there are major deficiencies, the contractor may be given 30 days to correct the deficiencies. If, after 30

days, the deficiencies remain, the contractor may be found in default and the contract cancelled.

6. Contracts Management Division (CMD) will forward the proposals of all offerors to the appropriate project officer for evaluation by a technical evaluation panel.

7. CMD will select the successful bidder and award the contract, contingent upon a satisfactory inspection of the contractor's facilities by OIG. CMD will notify the EPA Project Officer and OIG of its selection.

8. The Project Officer will ensure that the contractor is ready to be inspected by OIG and, when the contractor is ready, will notify OIG to perform the inspection.

9. OIG will inspect the contractor's facilities for compliance with the contractor security plan, including a review of the employee training awareness program, and inform ICB of the results.

10. If deficiencies are discovered during the course of the inspection, the contractor may be given 30 days to correct them. If after 30 days the deficiencies remain, the contractor may be found in default and the contract cancelled.

11. If the contractor facility is approved by ICB, ICB will notify the Project Officer and CMD.

12. The Project Officer will ensure that appropriate notice of data transfer to a contractor is given in accordance with 40 CFR Part 2. The Project Officer will arrange with the appropriate DCO/DCA for the transfer of the required CBI. The Project Officer will provide the DCO/DCA with the identity of the contractor, the number of the contract, a statement that the required clauses have been included in the contract, a copy of the approval by DAA/OTS.

13. When the TSCA CBI is furnished to the contractor, it will be handled in accordance with established procedures and a receipt will be obtained from the contractor DCO and given to the appropriate EPA DCO/DCA.

IV. Contractor Security Procedures

A. Security Plans

EPA's basic requirement is that the contractor's security plan must provide at least the same degree of protection for TSCA CBI as that provided by the *TSCA Confidential Business Information Security Manual*. Specific procedures must be set forth in the contractor security plan to cover each of the following areas.

1. *Authorization for Access*

Each contractor employee who will be receiving, handling, or storing TSCA CBI must:

- Be screened by a designated official of the contractor to ensure his/her honesty and trustworthiness.
- Be given written authorization for access to TSCA CBI by the designated official.
- Be fully informed of his/her responsibilities for the security and control of TSCA CBI before being given access to any document containing TSCA CBI.
- Sign a Contractor Employee Confidentiality Agreement (Appendix V) before receiving any TSCA CBI.

2. *Logging and Control of Documents*

All TSCA logs must be treated as CBI. The contractor must develop a logging and control system that includes the following elements.

- Appointment of a Contractor Document Control Officer (DCO) with overall responsibility for the system. The DCO must maintain a list of all authorized contractor personnel, along with a copy of their signed confidentiality agreements. The original of the signed confidentiality agreements will be forwarded to the Information Control Branch and will be the basis for listing employees on the EPA TSCA CBI Access List.
- An inventory log to record receipt and disposition of TSCA CBI from EPA or from another source.
- Procedures for the logging and control of TSCA CBI within the contractor facility. A system must be devised that includes a log with the name of the person using the information, the signature of the user, and document control number, the date checked out, and the date returned. All logs and other control documents, as well as copies of all the TSCA CBI, must be available for inspection and

copying by EPA. All logs must be returned to EPA at the end of contract performance.

- Assigning of a unique document control number to each document containing TSCA CBI and attaching a TSCA CBI cover sheet to every such document whenever these things have not already been done by EPA or the contractor.

- Ensuring that each page containing TSCA CBI is properly designated and marking the back of the last page of each TSCA CBI document. This requirement applies also to documents generated by the contractor or acquired from other sources.

3. *Storage*

a. *At the Contractor Facility*

The contractor must provide secure storage for TSCA CBI. The minimum acceptable storage container is a metal cabinet with a bar and a three-way changeable combination padlock of a type approved by EPA.

Combinations to all CBI storage containers must be controlled and issued only to authorized persons requiring access to the containers. A record of all combinations must be maintained by the contractor DCO, and each combination must be changed once each year or whenever an employee who knows the combination terminates or transfers, whichever comes first.

When the volume of TSCA CBI or other considerations warrant it, secure rooms or areas may be designated. Such rooms or areas should be equipped with combination-lock doors, special alarms, and other remote intrusion devices as required by the location, construction, and configuration of the room. Any such room must be inspected, prior to use, by the EPA OIG and approved by ICB.

b. *When Traveling*

With EPA permission, TSCA CBI may be taken home by authorized contractor employees prior to a trip when it would be impractical to return to the office to pick up the information. Contractor employees must take all reasonable measures to safeguard the information. When traveling by plane or other public conveyance, employees must keep TSCA CBI in their possession and may not check it with their luggage.

When a contractor employee is traveling with TSCA CBI (including samples) and is unable to deliver or ship the CBI to an authorized facility, TSCA CBI may be stored (for as short a period as possible) inside a locked container inside a locking portion of a motor vehicle. TSCA CBI may be stored in hotel safes.

4. *Transmittal*

TSCA CBI will usually be transmitted by registered mail, return receipt requested, in a double envelope. The inner envelope must reflect the name and

address of the recipient with the following additional wording on the front side: "TSCA CBI To Be Opened By Addressee Only." The outer envelope must reflect only the name and address without the additional wording.

When registered mail would take too long or other circumstances warrant it, the contractor may, with prior consent of the EPA Project Officer, use the Express Mail Service of the U.S. Postal Service, or private carriers previously approved by the ICB.

Physical samples collected by a contractor employee, such as those collected during a TSCA Inspection, which are claimed to be TSCA CBI, shall be placed in a package or container and the seal marked "TSCA Confidential Business Information." Such samples shall be delivered or shipped as soon as possible to the appropriate DCO/DCA in the Laboratory. If shipping or delivering is not immediately possible, as when an employee is traveling, the sample shall be stored inside a locked container inside a locking portion of a motor vehicle or in a hotel safe.

Authorized contractor personnel may hand-carry TSCA CBI to an EPA facility or to persons outside EPA (with the approval of the EPA Project Officer), providing the dispatching contractor DCO maintains a record and obtains a receipt from the person at the facility receiving the information. Information being hand-carried should be packaged as registered mail or in an alternate manner approved by ICB.

When circumstances warrant, and with OIG approval, special arrangements may be made for transporting TSCA CBI within a local area, e.g., the Washington, D.C., metropolitan area.

5. *Safeguards During Use*

When TSCA CBI is in actual use by an authorized person it must be kept under constant surveillance. The user must situate himself/herself in a physical position where he/she can exercise direct security control over the material. The material must be covered, turned face down, or otherwise protected when unauthorized persons are present.

6. *Destruction*

CBI documents provided the contractor by an EPA DCO/DCA may not be destroyed except with the permission of the providing EPA DCO/DCA. The contractor DCO shall remove the cover sheet, make a notation of the destruction on the cover sheet, and return it to the providing EPA DCO/DCA. Other TSCA CBI documents in the possession of the contractor may not be destroyed except with the permission of the EPA Project Officer or as specified in the security plan. Destruction must take place under the supervision of the contractor DCO by shredding or burning or other means approved by EPA. A record of destruction must be kept by the contractor in the appropriate log.

7. *Reproduction*

TSCA CBI may not be reproduced except upon approval by and under the supervision of the contractor DCO. Reproduction should be kept to an absolute minimum. The DCO must enter all copies into the document control system and apply the same control requirements to the copies as those for the original.

8. *Photographs*

Whenever it is necessary for a contractor employee to take photographs that contain TSCA CBI, as during a TSCA Inspection, either an "instant" camera must be used or the film must be processed by an authorized EPA photo lab or an authorized private photo lab contractor.

9. *Generating TSCA CBI Documents*

When a contractor employee generates a document that contains TSCA CBI, the newly generated document shall be taken as soon as possible to the contractor DCO, who shall enter it into the document control system and protect it as all other TSCA CBI. Generation of CBI documents by contractor employees shall be kept to a minimum. Documents generated from existing CBI documents shall be presumed to contain CBI and shall be treated as CBI until determined to be nonconfidential by EPA.

10. *Training of Employees*

The contractor's training program must be designed to fully inform all employees of their security responsibilities and of the consequences of any failure to comply with any requirements of the contractor security plan. Document control officers will require special training because of their unique responsibilities. Employees must be trained prior to gaining access to TSCA CBI. Records of employee attendance at training sessions and of the content of the training sessions must be kept and must be available to EPA upon request.

11. *Facility Security*

The contractor must provide a brief description of its facility, including location and physical security provisions for the building and the area where the TSCA CBI will be stored and used. This should include how building access is controlled (guards, alarms, locks, etc.) and any other pertinent security information.

12. *Lost or Unaccounted-for Documents*

Any lost or unaccounted-for document must be reported immediately to the EPA Project Officer or DCO/DCA, as appropriate, who shall forward a report to the ICB with a copy to the OIG.

13. *Incoming Mail*

Any incoming mail, whether from EPA, a business, or any other source, that contains TSCA CBI must be taken to the contractor DCO immediately to be entered into the document control system. Whenever there is reason to believe that a particular piece of mail may contain TSCA CBI, whether it is marked properly or not, that piece of mail should be taken to the DCO for opening and proper disposition.

14. *Telephone Calls*

With the approval of, and following guidelines provided by, the EPA Project Officer, authorized contractor employees may discuss TSCA CBI over the telephone with authorized EPA employees in Headquarters and other EPA offices. The contractor employee must verify that the EPA employee is authorized for access and must indicate at what point in the conversation TSCA CBI is to be discussed. In verifying that the EPA employee is authorized for access to TSCA CBI, the contractor employee will first check the access list, which will be maintained by the contractor DCO.

With the permission of the submitter, and after verifying his/her identity, authorized contractor employees may discuss TSCA CBI over the telephone with the submitter. If submitters discuss CBI over the telephone, employees shall notify them that such discussion does not constitute a waiver of any CBI claims.

15. *Secretarial Procedures*

Any person who is responsible for typing anything that contains TSCA CBI must be an authorized person. Typists are responsible for:

- Safeguarding the original and all "mag" cards, disks, one-time ribbons, drafts, scratch paper, notes, and any other materials that may contain TSCA CBI. No carbons or copies are to be made by the typists.

- Taking all reasonable measures to ensure that no unauthorized person can see or otherwise gain access to what he/she is typing.

- Protecting the materials at all times and storing them in approved containers when the work must be interrupted, such as at lunch or at close of business.

- Leaving nothing on the desk or in the typewriter (or word-processor, etc.) that might lead to the unauthorized disclosure of TSCA CBI. If the keyboard and printer are separate units, both must be under the direct physical control of the using employee. If a processing unit or storage medium is part of the system, and if either can be electronically or physically accessed by other persons, then the entire system must be approved by EPA prior to use. MIDSD may be asked for assistance in evaluating the security of the system.

- Taking the original and all other materials at the completion of the task to the author who will in turn take them to the DCO. The DCO will enter the original into the document control system and destroy all other material.

16. *Meetings*

For any meeting at which TSCA CBI will be discussed, the meeting chairperson shall provide a sign-in sheet if there are attendees who have not had prior access to the CBI to be discussed. In addition, the chairperson retains the option to require a sign-in sheet whenever he/she thinks it prudent. The sign-in sheet shall include the date, time, place, chairperson, and subject of the meeting. All attendees must sign it. The chairperson will give the sign-in sheet to the Contractor Document Control Officer who will retain it and return it to EPA at the end of contract performance.

The chairperson must ensure that only authorized persons are present and must announce that TSCA CBI is to be discussed. The chairperson must also review with the attendees their responsibility for safeguarding confidential business information in any and all forms, including, but not limited to, any notes taken and any subsequent discussions.

The chairperson must ensure that no recording is made of the meeting unless he/she has authorized it. If authorized, the recording must be treated as all other TSCA CBI and entered into the document control system.

Finally, the chairperson must ensure that the meeting room is secured after the meeting. This shall include cleaning all chalkboards, destroying all tear sheets and other notes, and ensuring that nothing is left in the room that could lead to the unauthorized disclosure of TSCA CBI.

B. Transfer of TSCA CBI to Contractor from EPA

The transfer of TSCA CBI to the contractor is initiated by the project officer responsible for the contract, who requests the required TSCA CBI from the appropriate EPA Document Control Officer (DCO) or Document Control Assistant (DCA). The request always includes the identity of the contractor, the number of the contract, a statement that the appropriate clauses are included in the contract, a copy of the approval given by the DAA/OTS, and a description of the CBI to be released. Upon receipt of such a request the DCO/DCA provides the requested information in accordance with established procedures.

The DCO/DCA then furnishes the information to the contractor in accordance with established procedures. The DCO/DCA obtains a written receipt for the information from the contractor and enters it into the log.

C. Notification of Affected Business

When required by 40 CFR Part 2, the program office shall notify each affected business in advance of any disclosure of TSCA Confidential Business Information.

D. Audits

Each contractor shall conduct periodic audits of its facilities, employees, and TSCA CBI security system to ensure compliance with its security plan. Records of such audits will be available to EPA OIG upon request.

E. Termination Inventory

At the completion of all contract work, the contractor shall conduct a complete inventory to ensure that all TSCA CBI is accounted for and furnish the results of the inventory to the EPA OIG and other EPA offices as directed.

F. Physical Security

Each contractor must have secure work areas where TSCA CBI is used. When not in use, for example, at lunchtime or at the close of business, TSCA CBI must be locked up in secure cabinets, safes, or special locked rooms. The minimum acceptable storage container is a metal cabinet with a bar and three-way changeable combination padlock of a type approved by EPA. The contractor must also have building or office security sufficient to prevent unauthorized entry.

G. Contractor-Acquired TSCA CBI

All of the above procedures shall apply when the contract requires the contractor to obtain TSCA CBI directly from any business. Any contract with this requirement must include the clause entitled Screening Business Information for Claims of Confidentiality (Appendix IV).

H. Return of TSCA CBI to EPA

Upon completion of the contract, the contractor shall return all TSCA CBI to the appropriate DCO/DCA. However, if the same information is needed in another unexpired contract with the same contractor, the DCO/DCA may instead obtain a written receipt for the information.

I. Additional Requirements

Any contract involving the use of TSCA CBI may include additional requirements, providing such requirements are as stringent or more stringent than those required by the EPA *TSCA Confidential Business Information Security Manual*.

V. Computer Security

A. Special Rules for Contractor Computer Use

If, under a proposed contract or a proposed modification to an existing contract, TSCA CBI is to be entered into the contractor's computer, the following additional security procedures must be enforced:

- Request for Approval of Contractor Access to TSCA CBI (Appendix VII) initiated by a Division Director (or equivalent) must specify the need for computer use.

- The offeror or contractor must develop and submit for review a Computer Center Security Plan addressing all of the computer security standards and procedures for EPA computers as specified in this chapter. Any deviation from these standards shall be identified in the Security Plan, along with a rationale explaining why the deviation would not significantly affect the level of security provided by the contractor.

- If the contractor will be developing an ADP application system that will process TSCA CBI, the contractor must also develop an ADP Application Security Plan in accordance with the requirements of this chapter.

- The OIG will review the Computer Center Security Plan and forward a report through ICB to the DAA/OTS. MIDSD will review the ADP Application Security Plan and recommend approval/disapproval to the DAA/OTS.

- If the DAA/OTS determines that these security plans would provide at least the same degree of protection as provided by the EPA procedures set forth in the *TSCA Confidential Business Information Security Manual*, he/she will approve the plans.

- In the case of an offeror, after such approval the offeror may be considered for the award of a contract.

- In the case of a proposal to modify an existing contract to include computer use, after such approval the contract may be so modified.

- The contract must include the clause entitled Computer Security (Appendix III).

- In no case will any TSCA CBI be transferred to the contractor for use in a computer until the contractor computer facility has been inspected by OIG and approved by ICB. When necessary, MIDSD may assist OIG on such inspections.

- The contractor must appoint a contractor computer DCO who will be responsible for all security aspects of the contractor's computer use

of TSCA CBI and who will log and control all use of the computer facilities.

The contractor must maintain records of computer use and make them available to EPA upon request by the EPA Project Officer. The contractor must also make its computer facilities available for inspection by EPA upon request by the EPA Project Officer.

B. Security Requirements for Contractor Computer Centers

1. *General*

In addition to the applicable Federal statutes and regulations cited in Chapter I. C. of the Manual, the computer processing of TSCA CBI must be in compliance with the following directives issued to all Federal agencies processing sensitive data by computer.

- Office of Management and Budget OMB Circular A71
- Office of Personnel Management FPM Ltr. 732-7
- National Bureau of Standards FIPS PUBS
- General Services Administration 41 CFR, Ch. 101

All TSCA contractor computer support facilities, whether dedicated to CBI processing or shared with non-CBI programs, must meet the basic requirements for protection of TSCA CBI.

a. *Basic Security Requirement*

The system must provide a level of security adequate to protect TSCA CBI that is being processed from unauthorized access by users and other persons having access to the facility.

b. *Computer Center Security Plan*

The contractor's computer DCO shall develop and maintain, a plan containing a comprehensive set of documented data security standards and procedures. This plan must include provisions for periodic risk analyses, provisions for obtaining confidentiality agreements from all contractor personnel working for the facility, such as equipment maintenance contractors, and provisions to meet all requirements specified below. This security plan shall be subject to approval by the DAA/OTS or his/her designee and shall be available to EPA OIG as required.

2. *Hardware and Software Characteristics*

a. *Hardware*

The computer hardware supporting the system shall be capable of maintaining isolation between user tasks, and shall prevent normal users from executing instructions reserved for the operating system. Since a well-designed system of software, as specified below, can adequately compensate for many desirable hardware features, no further specific hardware requirements are set forth here.

b. *Software System Design*

The operating system software shall have data security as one of its primary design requirements. This operating system shall provide mechanisms to implement the following principles.

Note that the software system design requirements discussed below are essentially identical to the hardware requirements specified above and may be substituted for the hardware requirements if proven effective. The requirements are:

- *User/Task Isolation*--Separate users or tasks operating concurrently in the system shall be, within system limits, totally isolated from one another.

- *Control of Interfaces and Security Sensitive Work Spaces*--Operating system interfaces shall prevent users from gaining access to instructions or data reserved for the operating system. The operating system shall not use user-accessible work areas for passwords or other system sensitive data.

- *Audit Trails*--The system shall provide extensive auditing data to record significant system activities that are of a security concern, such as log-on attempts, file accesses, and program execution. The system shall provide to EPA a list of all attempts at unauthorized access of EPA or contractor data files and/or programs by users and others.

- *User Identification and Authorization*--There shall be mechanisms in the operating system to identify individual users of the system and to specify the system resources and privileges to which the user is authorized.

c. *Applications Software Management*

Any employee responsible for developing software that will process TSCA CBI is required to prepare an ADP Application Security Plan. This plan shall describe the components of the system or subsystems that may be accessible by authorized DCOs and DCAs including computer programs, inputs, outputs, and data bases. The plan shall also state how this security is to be enforced,

and, in particular, how unauthorized modifications to the programs will be prevented. The plan must address controls to ensure data integrity and systems assurance, including audit trails. The plan must be reviewed and approved by the DAA/OTS or his/her designee, following review by the Director of the Management Information and Data Systems Division, and the Inspector General. The program instituted must be periodically reviewed for effectiveness and shall be subject to periodic audit.

d. *File-Catalog Structure*

The operating system shall provide resource control at the file level that permits isolation of one user's files from another's. It shall not be possible for one user to access another's files simply by having knowledge of the file name and account number.

e. *File Access Control/Permission Mechanism*

The operating system shall provide for file access through a specific permission mechanism capable of:

- *Specific User Permissions*--It must be possible to give selected users access to a particular file without giving all users access to the file.

- *Access Type Control*--It must be possible for a file owner to restrict the type of access to a file. Two minimum categories must be supported: Read Only Access and Read/Write Access. Additionally, it is highly desirable that it be possible to restrict access to program files on an execute only (i.e., no read) basis, and to restrict "control" access to files (i.e., scratching or renaming the file).

f. *User Features*

To enable user flexibility in adding security features to applications, the system should provide a range of optional protection features, including:

- *Password Change Capability*--Individual users (DCOs and DCAs authorized for computer access) should ensure that their own log-on and file-access passwords are changed at frequent intervals.

- *Idle Terminal Disconnect*--The system should provide a mechanism to automatically disconnect a user terminal after a fixed period of no activity. If the terminal is a CRT type, then the system should clear the screen before the automatic disconnect.

g. *Communications Facilities*

The communications network must be adequately protected against intentional or accidental misrouting of data traffic. Line protocol and concentrator-modem interfaces must be designed to detect and protect against anomalous events

(such as spurious data or line disconnects) that might otherwise cause misrouting or loss of data.

Communications equipment (modems, multiplexors, concentrators, etc.) shall be located in secure areas accessible only to authorized personnel.

When TSCA CBI is transmitted electronically through communications lines, such lines must be protected in accordance with the National Bureau of Standards' Data Encryption Standards. Such encryption is not required for hardwired connections within a secure facility.

Any terminal or printer used to read or print TSCA CBI must be located in a secure room and used for this purpose only by a person with computer access authorization.

3. *Media Handling*

Policies and procedures must be included in the security plan to fully control access to and handling of various data media used in processing TSCA CBI including magnetic tape, disk packs, printed output, cards, micrographic output, and other such media.

Media shall be labeled only with such information as is necessary for retrieval and media management.

Storage areas for various media, including mountable volumes, should be separate from the main operations areas.

Input and output media shall be transmitted only between the computer DCO and the appropriate program area DCO. In no case shall input media be accepted from or delivered to a third party. Positive user identification procedures must be in effect. Detailed logs of all media transmitted to and from the computer facility shall be maintained.

When authorized in writing by a DCO, media shall be disposed of by the computer DCO in a manner that will prevent any disclosure of data to outside parties.

4. *Facility Protection*

All necessary steps must be taken to protect facilities, equipment, and the data they contain from inadvertent or intentional access, damage, or destruction.

The computer DCO shall enforce a policy of permitting no unescorted visitors into computer operations areas or into areas where sensitive data are handled. Only designated personnel having an ongoing need shall be authorized unescorted access to such areas.

Any computer facility processing TSCA CBI must have, prior to receiving such data, an adequate facility or building security system to protect the equipment and data approved by the ICB.

5. *Backup and Recovery Capability*

There shall be documented procedures to ensure adequate backup and recovery capability in the event of loss of data or processing capability through accident or disaster. These procedures should include a provision for periodic testing of the backup and recovery capabilities.

All files resident on the system shall be copied to backup media on a regular basis.

A complement of backup files that will enable recovery to the previous end-of-week position in the event of a major disaster resulting in loss of on-site copies shall be stored off-site. An off-site storage facility is defined as one that is so located that it is highly unlikely to be affected by a major disaster (fire, explosion, etc.) striking the main facility. Off-site storage shall be as secure as that at the primary location of data and shall be approved by the ICB.

Appendix I

The Contracting Officer has determined that during the performance of this contract, EPA may furnish confidential business information to the Contractor that EPA obtained under the Clean Air Act (2 U.S.C. 1857 et seq.), the Federal Water Pollution Control Act (33 U.S.C. § 1251 et seq.), the Safe Drinking Water Act (42 U.S.C. § 300f et seq.), the Federal Insecticide, Fungicide, and Rodenticide Act (7 U.S.C. § 136 et seq.), the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 301 et seq.), the Resource Conservation and Recovery Act (42 U.S.C. § 2901 et seq.), or the Toxic Substances Control Act (15 U.S.C. § 2601 et seq.). EPA regulations on confidentiality of business information in 40 CFR Part 2 Subpart B require that the Contractor agree to the clause entitled "Treatment of CBI" before any confidential business information may be furnished to the Contractor.

Treatment of Confidential Business Information

A. The EPA Project Officer, after a written determination by the appropriate program office, may disclose confidential business information to the Contractor necessary to carry out the work required under this contract. The Contractor agrees to use the confidential information only under the following conditions:

1. The Contractor and Contractor's Employees shall: (i) use the confidential business information only for the purposes of carrying out the work required by the contract; (ii) not disclose the information to anyone other than EPA employees without the prior written approval of the Deputy Associate General Counsel for Contracts and General Administration; and (iii) return to the Contracting Officer all copies of the information, and any abstracts or excerpts therefrom, upon request by the Project Officer, whenever the information is no longer required by the Contractor for the performance of the work required by the contract, or upon completion of the contract.

2. The Contractor shall obtain a written agreement to honor the above limitations from such of the Contractor's Employees who will have access to the information, before the employee is allowed access.

3. The Contractor agrees that these contract conditions concerning the use and disclosure of confidential business information are included for the benefit of, and shall be enforceable by, both EPA and any affected business having a proprietary interest in the information.

4. The Contractor shall not use any confidential business information supplied by EPA or obtained during performance hereunder to compete with any business to which the confidential information relates.

B. The Contractor agrees to obtain the written consent of the Contracting Officer, after a written determination by the appropriate program office,

prior to entering into any subcontract that will involve the disclosure of confidential business information by the Contractor to the subcontractor. The Contractor agrees to include this clause, including this paragraph (B), in all subcontracts awarded pursuant to this contract that require the furnishing of confidential business information to the subcontractor.

Appendix II

The Contracting Officer has determined that during the performance of this contract, EPA may furnish confidential business information to the Contractor that EPA has obtained under the Toxic Substances Control Act (15 U.S.C. § 2601 et seq.). The Contractor must agree to this clause entitled "Security Requirements for Handling TSCA Confidential Business Information" before any confidential business information obtained under the Toxic Substances Control Act may be furnished to the Contractor. The clause entitled "Treatment of Confidential Business Information" is also included in this contract.

Security Requirements for Handling

TSCA Confidential Business Information

A. The Project Officer, after a written determination by the appropriate program office, may disclose confidential business information to the Contractor necessary to carry out the work required under this contract. The Contractor agrees to protect the confidential business information in accordance with the following requirements:

1. The Contractor and Contractor's Employees shall follow the security procedures set forth in the contractor security plan(s) approved by EPA.

2. The Contractor shall permit access to and inspection of the Contractor's facilities in use under this contract by representatives of EPA's OIG.

3. The Contractor DCO shall obtain a signed copy of the "TSCA Contractor Employee Confidentiality Agreement" from each of the Contractor's Employees who will have access to the information, before the employee is allowed access.

B. The Contractor agrees that these requirements concerning protection of confidential business information are included for the benefit of, and shall be enforceable by, both EPA and any affected business having a proprietary interest in the information.

C. The Contractor understands that confidential business information obtained by EPA under the Toxic Substances Control Act may not be disclosed except as authorized by the Act and that any unauthorized disclosure by the Contractor or the Contractor's Employees may subject the Contractor and the Contractor's Employees to the criminal penalties in section 14(d) of the Act. For purposes of this contract, the only disclosures that EPA authorizes the Contractor to make are those disclosures set forth in the clause entitled "Treatment of Confidential Business Information."

D. The Contractor agrees to include this clause, including this paragraph (D), in all subcontracts awarded pursuant to this contract that require the furnishing of confidential business information to the subcontractor.

E. The Contractor shall return all logs and employee confidentiality agreements to EPA at the end of the contract.

Appendix III

The Contracting Officer has determined that during the performance of this contract, EPA may furnish to the Contractor confidential business information that EPA has obtained under the Toxic Substances Control Act (15 U.S.C. § 2601 et seq.). The Contractor will use this confidential business information in a computer. The Contractor must agree to this clause entitled "Computer Security" before any confidential business information obtained under the Toxic Substances Control Act may be furnished to the Contractor. The clause entitled "Security Requirements for Handling TSCA Confidential Business Information" is also included in this contract.

Computer Security

A. The Contractor agrees to protect confidential business information used in its computer operations in accordance with the following requirements:

1. The Contractor and the Contractor's Employees shall follow the computer security procedures set forth in the Computer Center Security Plan and/or ADP Application Security Plan proposed by the Contractor and accepted by EPA.

2. The Contractor and the Contractor's Employees shall follow the procedures required by the clause entitled "Security Requirements for Handling TSCA Confidential Business Information" of this contract for all confidential business information removed from the computer.

3. The Contractor shall, upon request by EPA, permit access to and inspection of the Contractor's computer facilities in use under this contract by representatives of EPA's OIG and EPA's Management Information and Data Systems Division.

B. The Contractor agrees that these requirements concerning computer security of confidential business information are included for the benefit of, and shall be enforceable by, both EPA and any affected business having a proprietary interest in the information.

C. The Contractor agrees to include this clause, including this paragraph (C), in all subcontracts awarded pursuant to this contract that require use of confidential business information in computers.

Appendix IV

The Contracting Officer has determined that during performance of this contract the Contractor may be required to collect information to perform the work required under this contract. Some of the information may consist of trade secrets or commercial or financial information that would be considered as proprietary or confidential by the business that has the right to the information. The following clause is included in this contract to enable EPA to resolve any claims of confidentiality concerning the information that the Contractor will furnish under this contract. The clause entitled "Treatment of Confidential Business Information" is also included in this contract.

Screening Business Information for Claims of Confidentiality

(a) Whenever collecting information under this contract, the Contractor agrees to comply with the following requirements:

(1) If the Contractor collects information from public sources, such as books, reports, journals, periodicals, public records, or other sources that are available to be public without restriction, the Contractor shall submit a list of these sources to the appropriate program office at the time that information is initially submitted to EPA. The Contractor shall identify the information according to source.

(2) If the Contractor collects information from a State or local government or from a Federal agency, the Contractor shall submit a list of these sources to the appropriate program office at the time the information is initially submitted to EPA. The Contractor shall identify the information according to source.

(3) If the Contractor collects information directly from a business or from a source that represents a business or businesses, such as a trade association:

(i) Before asking for the information, the Contractor shall identify itself, explain that it is performing contractual work for the U.S. Environmental Protection Agency, identify the information that it is seeking to collect, explain what will be done with the information, and give the following notice:

(A) You may, if you desire, assert a business confidentiality claim covering part or all of the information. If you do assert a claim, the information will be disclosed by EPA only to the extent and by means of the procedures set forth in 40 CFR Part 2 Subpart B, 41 FR 36906, September 1, 1976.

(B) If no such claim is made at the time this information is received by (the Contractor), it may be made available to the public by the Environmental Protection Agency without further notice to you.

(ii) Upon receiving the information, the Contractor shall make a written notation that the notice set out above was given to the source, by whom, in what form, and on what date.

(iii) At the time the Contractor initially submits the information to the appropriate program office, the Contractor shall submit a list of these sources, identify the information according to source, and indicate whether the source made any confidentiality claim and the nature and extent of the claim.

(b) The Contractor shall keep all information collected from nonpublic sources confidential in accordance with the clause in this contract entitled "Treatment of Confidential Business Information" as if it had been furnished to the Contractor by EPA.

(c) The Contractor agrees to obtain the written consent of the Contracting Officer, after a written determination by the appropriate program office, prior to entering into any subcontract that will require the subcontractor to collect information. The Contractor agrees to include this clause, including this paragraph (c), and the clause entitled "Treatment of Confidential Business Information" in all subcontracts awarded pursuant to this contract that require the subcontractor to collect information.

Appendix V

TSCA CONTRACTOR EMPLOYEE CONFIDENTIALITY AGREEMENT

I understand that as an employee of _____, a contractor performing work for the United States Environmental Protection Agency, I will have access to certain TSCA Confidential Business Information submitted under the Toxic Substances Control Act (TSCA) (15 U.S.C. Section 2601 et seq.). This access has been granted to me in order to perform my work under the contract.

I understand that TSCA Confidential Business Information may not be disclosed by me except as authorized by TSCA, the contract, and the security procedures used by my company under the contract. I understand that under Section 14 (d) of TSCA (15 U.S.C. Section 2613 (d)), I am liable for a possible fine of up to $5,000 and/or imprisonment for up to one year if I willfully disclose TSCA Confidential Business Information to any person not authorized to receive it. In addition, I understand that I may be subject to disciplinary action for violation of this agreement up to and including dismissal.

I agree that I will treat any TSCA Confidential Business Information furnished to me as confidential and that I will follow the security procedures used by my company under the contract. I have been informed of and understand the procedures.

TYPED NAME AND SIGNATURE OF CONTRACTOR EMPLOYEE	DATE

EPA Form 7710-19 (Rev. 9/81)

Appendix VI

CONFIDENTIALITY AGREEMENT FOR CONTRACTOR EMPLOYEES UPON TERMINATION OR TRANSFER

As an employee of , a contractor performing work for the United States Environmental Protection Agency, I have had access to certain confidential business information submitted under the Toxic Substances Control Act (TSCA) (15 U.S.C. Section 2601 et seq.). This access was granted to me in order to perform my work under a contract.

I certify that I have returned all copies of any TSCA Confidential Business Information in my possession to the appropriate document control officer specified in the security plan in effect at my company.

I agree that I will not remove any copies of TSCA Confidential Business Information from the premises of the company upon my termination or transfer. I further agree that I will not disclose any TSCA Confidential Business Information to any person after my termination or transfer.

I understand that as a contractor employee who has had access to TSCA Confidential Business Information, under Section 14 (d) of TSCA (15 U.S.C. Section 2613 (d)) I am liable for a possible fine of up to $5,000 and/or imprisonment for up to one year if I willfully disclose TSCA Confidential Business Information to any person.

If I am still employed by the contractor, I also understand that I may be subject to disciplinary action for violation of this agreement.

I am aware that I may be subject to criminal penalties under 18 U.S.C. Section 1001 if I have made any statement of material facts knowing that such statement is false or if I willfully conceal any material fact.

TYPED NAME AND SIGNATURE OF CONTRACTOR EMPLOYEE	DATE

EPA Form 7710-43 (9/81)

Appendix VII

(Front)

(Actual Size 8 1/2" x 11")

REQUEST FOR APPROVAL OF CONTRACTOR ACCESS TO TSCA CONFIDENTIAL BUSINESS INFORMATION

Requesting Official*	Signature	Date

Title and Office

Contractor and contract number (if modification)

I. Brief description of contract, including purpose, scope, length, and other important details. (Continue on the back of this form if necessary.)

II. What TSCA CBI will be required, and why? (Continue on back if necessary.)

III. Will computer access to TSCA CBI be required by the contract? If so, explain why and to what extent on the back of this form.

If you approve this request, this office will initiate procedures to ensure compliance with the "TSCA CBI Security Manual" and "Contractor Requirements for the Control and Security of TSCA Confidential Business Information."

***Must be Division Director (or equivalent) or above.**

Office Director for Toxic Substances

Approved _____

Date _____

EPA Form 7710-15a (9-81)

Appendix VII

(Back)

(Actual Size 8 1/2" x 11")

I. (Continued)

II. (Continued)

III. (Continued)

EPA Form 7710-15a (9-81) Reverse

Index

	Page
Access, Defined	2
Access, How To Gain	11
ADP Application Security Plan	
Defined	2
Audits	17
Authorized Computer Facility	
Defined	2
Authorized Person, Defined	3
Backup Capability	24
Computer Center Security Plan	
Defined	3
Discussed	20
Computer Security	19
Confidential Business Information (CBI), Defined	3
Contractor	3,7
Contractor DCO	
Defined	3
Responsibilities of	7
Contracts Management Division	5
DAA/OTS, Responsibilities of	5
Destruction	13
Director, MIDSD, Responsibilities of	6
Division Directors, Responsibilities of	5
Document Control Officer, DCO, EPA, Defined	3
Document, Defined	3
Documents, Lost	14,24
Employees, Contractor, Responsibilities of	8
Facility Protection	23
Facility Security	14
Hardware Requirements	21
Information, Defined	3
Logging of Documents	11
Lost Documents	14,24
Mail	15
Media Handling	23
Meetings	16

B161
9

Index (cont.)

	Page
Notes	16
Office of the Inspector General	
Responsibilities of	6
Penalties, Criminal	1
Policy, EPA	1
Procedures, Award	9
Project Officer (EPA)	
Defined	3
Responsibilities of	6
Recovery Capability	24
Reproduction	14
Safeguards During Use of TSCA CBI	13
Secretarial Procedures	15
Secure Facility, Defined	3
Secure Room, Defined	4
Security Plans	
Defined	4
Discussed	4
Security Violations	2
Software System Design	21
Storage	12
Telephone Calls	15
Termination Inventory	17
Training of Employees	14
Transmittal	12
Travel	12
TSCA	1
Typing Procedures	15
Violations	
Appropriate Action by DAA/OTS	2
Defined	4
Penalties for	1
of Contracts	6
Reporting of, by Contractors	2
Reporting of, by DCOs	7
Reporting of, by Employees	8

*U.S. GOVERNMENT PRINTING OFFICE 341-082/255